

# Security against jamming and noise exclusion in imaging

Wojciech Roga and John Jeffers\*

*SUPA, Department of Physics, University of Strathclyde, John Anderson Building, 107 Rottenrow,  
Glasgow G4 0NG, UK*

September 12, 2016

## Abstract

We describe a protocol by which an imaging system could be protected against jamming by a malevolent party. Our protocol not only allows recognition of the jamming, but also allows for the recovery of the true image from the jammed one. We apply the method to jamming of quantum ghost imaging, for which the jamming detection probability is increased when the imaging light is entangled. The method can also be used to provide image recovery in general noisy environments.

## 1 Introduction

Image security is a challenge that arises when spatial information about an object is transferred to and imaged by a device at a remote location. It is more important when receiving particular images implies related actions. Security cannot normally be guaranteed along the entire path between the source of light and the detectors. Imagine a situation in which an intruder places a false object in front of the real one, or alternatively changes the path of a beam to direct it via a false object. There is no protection from such tampering. Thus when we simply point a camera we can not be sure whether or not the light received bears any relation to any real object. Someone may simply send us the image that they want us to see. Of course we can provide more confidence by controlling of the source of radiation as well as the detector, as is done in radar or lidar systems, but the fundamental point is that imaging is insecure.

Quantum protocols have been applied to imaging and communication, providing several advantages [1, 2, 3, 4, 5, 6]. Among them are detection of imaging jamming and appropriate protection [7, 8]. In communication situations we can use encryption to safeguard information in transit. This typically relies on secure key-sharing protocols, an example of which is quantum key distribution [9, 10, 11, 12]. When this procedure succeeds two parties share a secret key and only limited private information can leak to an eavesdropper. In imaging, however, the privacy condition is not normally crucial. We simply care that the image received exactly corresponds to the object. This is an example of public communication in which we stress the correctness of the message or image instead of its privacy. We face not an eavesdropper but an active intruder, who may already know the object and, instead, wants to jam the imaging protocol, changing information and consequently perhaps a strategic decision.

As already stated, there is no secure protection from an intruder who uses a false object or a false beam path. It may, however, be difficult for the intruder to perform such jamming both efficiently and undetectably. Thus we investigate a weaker jamming procedure in which some of the light from a trusted source of illumination is intercepted by the intruder and replaced by light from their independent source [13, 14, 15]. As the party who prepares states of light has naturally more information about the states than it is possible to extract from a measurement, the legitimate imager has an informational advantage over the intruder. This advantage can be a source of imaging security as we show in this paper.

The paper is organised as follows. In Sec. 2, we analyse the general image security scenario and provide a universal description of intruder detection and correct image recovery. Our protocol applies to both deliberate jamming and to image noise. In Sec. 3, we define a quantitative criterion for image comparison that enables us to estimate the probability that we detect jamming and a false alarm probability. In Sec. 4, we propose an arrangement of ghost imaging [1, 16, 19, 17, 18] protected against such jamming by using both classical and quantum-correlated light. Here, we show an advantage of using the quantum-correlated light and demonstrate the recovery protocol. Finally, concluding remarks and possible extensions of these work are discussed in Sec. 5.

---

\*Corresponding author: wojciech.roga@strath.ac.uk

## 2 Universal intrusion detection and image recovery protocol

Let us start with a general description of imaging protected by a security system that allows us to both detect the presence of an intruder and to counter the effect of jamming. We note at the outset that there is nothing specifically quantum about our procedure. It can be performed with classical light. There can sometimes be advantages, however, to using certain types of quantum state.

We assume that states of light  $\rho(\mathbf{x}, \kappa)$  used to image an object are characterized by spatial coordinates  $\mathbf{x}$  describing the coordinates of light during the procedure together with another degree of freedom  $\kappa$  that is used to detect intrusion and recover the image. In this paper  $\kappa$  denotes a polarisation state, however all the results could apply to other degrees of freedom. Suppose that states produced by a trusted source interact with an object and therefore carry information about it. These states are denoted  $\rho_j(\mathbf{x}, \kappa)$ , where  $j$  indicates that the legitimate imager can choose from a set containing more than one state of light for imaging. Indeed, this diversification is crucial to the protocol.

An intruder intercepts a fraction  $r$  of the light and resends their own photons in state  $\rho^E(\mathbf{x}, \kappa')$ . Superscript  $E$  refers to an intruder or jammer or simply a noisy environment that introduces errors. We assume that the state selected by the intruder does not depend on the choice of  $j$  made randomly by the imagers and is, at least on average, constant in time. This is a reasonable assumption because in imaging the dynamics of the process is not typically relevant. We will discuss this condition further in the context of particular implementations. In the final part of the paper we comment on the situation in which it is partially relaxed, i.e. the state of the intruder changes in time in such a way that a partial correlation between  $\rho^E(\mathbf{x}, \kappa')$  and  $j$  is established.

The intrusion detection and image recovery arrangement contains a set of polarisation analysers. The analysing system induces the detectors to make a measurement of  $\kappa$  by filtering, characterised by a set of parameters  $\{\theta_i\}$ , which in our case denotes the set of angles of different polarisers. We consider a general situation of multi-photon coincidence imaging with  $n$  photons involved in which  $i = 1, \dots, n$ . A spatial distribution of intensities in an image is proportional to probabilities corresponding to an  $n$ -photon polarisation state  $\rho = \rho(\mathbf{x}, \kappa)$  which depend on the analyser angles  $\theta_i$  and are given by

$$P(\{\theta_i\}, \rho) = \left( \langle a(\theta_1) | \otimes \dots \otimes \langle a(\theta_n) | \right) \rho \left( | a(\theta_1) \rangle \otimes \dots \otimes | a(\theta_n) \rangle \right). \quad (1)$$

This is a probability if  $\rho$  is a state with exactly  $n$ -photons, otherwise it is an expectation value. Here, for a single analyser and fixed basis of horizontal-vertical polarisations,  $|a(\theta_i)\rangle = \cos \theta_i |\leftrightarrow\rangle + \sin \theta_i |\updownarrow\rangle$ . The state of the entire system, before any action of the analysers can be written as  $(1-r)\rho_j + r\rho^E$ . The intensity distributions of images are proportional to

$$(1-r)P(\{\theta_i\}, \rho_j) + rP(\{\theta_i\}, \rho^E). \quad (2)$$

Here several images indexed by  $j$  and  $i$  are obtained. If the intensity dependence of the received images corresponds to the distribution  $P(\{\theta_i\}, \rho_j)$ , which is known only to the imager, then we can infer that there is no intrusion. If not, intrusion is detected and, if it is only partial ( $r < 1$ ), the correct image can be recovered, as we now show.

As an example assume that imager uses two different states of polarisation, so  $j = 1, 2$ . The contribution of the intruder  $\rho^E$  does not depend on  $j$  so the detected images  $(1-r)P(\{\theta_i\}, \rho_1) + rP(\{\theta_i\}, \rho^E)$  and  $(1-r)P(\{\theta_i\}, \rho_2) + rP(\{\theta_i\}, \rho^E)$  have the same contribution to the image induced by the intruder. If the contribution from  $P(\{\theta_i\}, \rho_1)$  is different to the contribution from  $P(\{\theta_i\}, \rho_2)$  the absolute value of the difference between the two images for any  $i$  eliminates any incorrect part of the image while merely attenuating any correct part because the difference of the images is taken. This procedure allows us to distill a correct, although attenuated, image of the investigated object.

## 3 Quantitative comparison of images

### 3.1 Probability of jamming detection

An essential part of the detection protocol is based on the ability of legitimate imagers to distinguish between images formed by two kinds of state characterised by different polarisation degrees of freedom. In order to compare images quantitatively we define a *state dependent visibility*  $V$  that for given pair of polarisation states  $\rho_1$  and  $\rho_2$  and for a given set of analyser orientation angles  $\{\theta_i\}$  is given by

$$V(\rho_1, \rho_2, \{\theta_i\}) = \frac{|P_1 - P_2|}{P_1 + P_2}, \quad (3)$$

where  $P_1$  and  $P_2$  are photon detection probabilities for states  $\rho_1$  and  $\rho_2$  respectively as in (1). Although, for brevity, we omit the arguments of  $P_j$  in our notation, we assume that  $P_j = P_j(\{\theta_i\}, \rho_j)$  i.e.  $P_j$  is defined for a specific state

and for a chosen set of analyser angles. Notice that for  $\rho_1 = \rho_2$  the state dependent visibility vanishes, showing that the images are identical. If, instead, for two different states  $V \neq 0$  it means that intensity distributions of two images are different.

As the legitimate imagers know both the states used and the analyser orientations in ideal conditions without intrusion they expect to observe images of a particular state dependent visibility. Any noise or intrusion will reduce the observed visibility.

The measured and expected visibilities provide data for hypotheses testing based on the likelihood ratio test [20, 13]. Our null hypothesis  $H_0$  assumes no intruder while the alternative hypothesis  $H_1$  assumes the presence of intercept-resend jamming. We must also account for real devices having some level of noise. Let us assume that the measured visibilities are associated with the Gaussian noise of variance  $\sigma$  and test the hypotheses based on the likelihood ratio test with prior probabilities 0.5 (and the test threshold  $\lambda = 1$ ). Visibilities related to the two hypotheses are the following: for  $H_0$  we have  $s_0 = V_0 + N$  and for  $H_1$ ,  $s_1 = V_1 + N$  where  $V_0$  and  $V_1$  are the average values of the visibilities and  $N$  is the Gaussian noise with variance  $\sigma$ . In the log-likelihood ratio test we decide that  $H_0$  occurs if

$$\sum_i \tilde{s}_i < \frac{\ln \lambda}{d} + \frac{d}{2}, \quad (4)$$

where  $\tilde{s}_i = s_i/(\sigma\sqrt{M})$ , and  $M$  is a number of trials which we will assume to be 1. Here  $d = \sqrt{M}(V_1 - V_0)/\sigma$ . A corresponding inequality to Ineq. (4) convinces us to accept  $H_1$ . The probability of correct detection of an intruder (i.e. when  $H_1$  is correctly accepted) and the false alarm probabilities are

$$P_d = \text{erfc} \left[ \frac{\ln \lambda}{d} - \frac{d}{2} \right], \quad (5)$$

$$P_{\text{err}} = \text{erfc} \left[ \frac{\ln \lambda}{d} + \frac{d}{2} \right], \quad (6)$$

and  $\text{erfc}[x]$  denotes the complimentary error function [20].

### 3.2 Application of the detection strategy, level of jamming

In order to demonstrate the optimal decision strategy made by the legitimate imagers let us consider the attack in which the intruder intercepts a fraction  $r$  of the original photons and replaces them with photons in a state  $\rho^E$  carrying the false image.

As the intruder detection probability (5) is a monotonic function of the difference between expected and observed state dependent visibilities, the intruder will choose states carrying false information such that this difference is as small as possible. The legitimate imagers have freedom in the choice of analyser angles and will want to maximise this difference. In principle, the intruder could optimize their state for each value of  $\{\theta_i\}$ . Although it is unlikely, the legitimate imagers can consider this situation in order to check the robustness of their state choice against jamming. Thus they are able to decide the states for which the detectability of an intruder is largest. Hence in the worst case scenario the detection probability (5) is a monotonic function of

$$d = \frac{1}{\sigma} \max_{\{\theta_i\}} \left[ \min_{\rho^E} \left( V(\rho_1, \rho_2, \{\theta_i\}) - V(\rho'_1, \rho'_2, \{\theta_i\}) \right) \right], \quad (7)$$

where  $\rho_1$  and  $\rho_2$  are the states chosen by the legitimate imagers and

$$\rho'_j = (1 - r)\rho_j + r\rho^E, \quad \text{where } j = 1, 2 \quad (8)$$

are the states carrying false information. The parameter  $d$  is estimated for a given level of intrusion. In cryptography a similar parameter is given by a secrecy function [21]. For image comparison we introduce the *level of jamming* in terms of the state dependent visibility for jammed and non-jammed images

$$V_L = \max_j V(\rho_j, \rho'_j, \{\theta_i\}), \quad (9)$$

where  $\rho_j$  means the state from legitimate source and  $\rho'_j = (1 - r)\rho_j + r\rho^E$  its jammed counterpart. The level of jamming  $V_L$  quantitatively describes how at most the actual image can differ from the correct one in visibility. In principle, as a measure of the intrusion level we could consider the intercepting rate  $r$ . However, this is not the optimal choice, as even for large  $r$  the correct image may be attenuated but not changed as is shown in the following example.

*Example. One photon states.* Imagine that the states chosen by legitimate parties are  $\rho_1 = |\leftrightarrow\rangle\langle\leftrightarrow|$  and  $\rho_2 = |\uparrow\rangle\langle\uparrow|$ . We assume that  $\rho^E$  can be an arbitrary one photon polarisation pure state  $\rho^E = |\phi\rangle\langle\phi|$ , where  $|\phi\rangle = \cos\alpha|\leftrightarrow\rangle + e^{i\beta}\sin\alpha|\uparrow\rangle$ , for arbitrary real  $\alpha$  and  $\beta$ . It is easy to show that in this case

$$V(\rho'_1, \rho'_2, \theta) = \frac{(1-r)V(\rho_1, \rho_2, \theta)}{1-r+r\langle a(\theta)|\rho^E|a(\theta)\rangle}, \quad (10)$$

where  $\rho'_i$  are given by

$$\rho'_j = (1-r)\rho_j + r\rho^E, \quad \text{where } j = 1, 2. \quad (11)$$

Thus for each  $\theta$  the intruder can find a state  $\rho^E$  orthogonal to  $|a(\theta)\rangle$ . Hence, for any intercepting rate  $r$  the parameter  $d = 0$  and the probability of detection is as small as possible, equal to the probability of an unbiased guess 0.5. However, notice that although the interference of the intruder is significant, the image is not changed apart from being attenuated. Because we stress the correctness of the image rather than its intensity, which we do not fully control, this invasion is not treated as jamming. Therefore, we do not treat  $r$  as a proper characterisation of the degree of jamming.

## 4 Ghost imaging jamming

In ghost imaging correlations between photons in two separate light beams, which we call the object beam and the image beam, allow an image of an object to be obtained by detecting light that has never interacted with it directly. The object beam interacts with an object with a particular spatial profile. This beam is detected with a bucket detector that provides no spatial information. The image beam does not interact with the object but falls on a spatially resolving detector. An image appears at this detector due to coincidence correlations between two detectors. The technique has applications for example, for difficult to access objects where a single pixel detector might be easier to place, or if it is easier to detect spatial images at one wavelength rather than another [17, 18]. The correlations also provide timing information.

### 4.1 Probability of jamming detection in ghost imaging

In what follows we describe the detection and recovery protocol applied to ghost imaging. This two-photon coincidence imaging allows us additionally to show that imaging with entangled states can increase the probability of intrusion detection compared to classically correlated states.

A ghost imaging setup contains the following fundamental elements: a source of correlated photons,  $S$ , the investigated object,  $\Lambda$ , a bucket detector  $D_L$  and a spatially-resolving detector  $D_R$ . These elements are shown in Fig. 1 which is arranged in the so-called Klyshko picture [22, 23]. The central part of the setup is doubled, showing the symmetric role of imagers (lower) and an intruder (upper). Polarisation analysers  $P_1$  and  $P_2$  can be rotated independently to distinguish two angles  $\theta_1$  and  $\theta_2$  of polarisation filtering. Intruder  $E$  intercepts a fraction of the photons sent by trusted source  $S$  and resends pairs of photons, correlated in polarisation, which carry false image information. We assume that different photons from each pair travel through different arms and  $E$  intercepts photons from only one arm. This is enough to prevent coincidence counting which can contribute to a correct image.

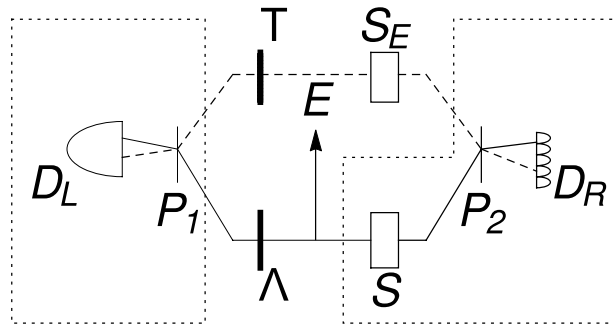


Figure 1: Ghost imaging with security. Intruder  $E$  intercepts part of a signal emitted by source  $S$  sent to an object  $\Lambda$ .  $E$  re-sends correlated pairs of photons produced by source  $S_E$  that carry information about a false object  $T$  to both right and left detectors. Regions bordered by dotted lines denote zones controlled by imagers.

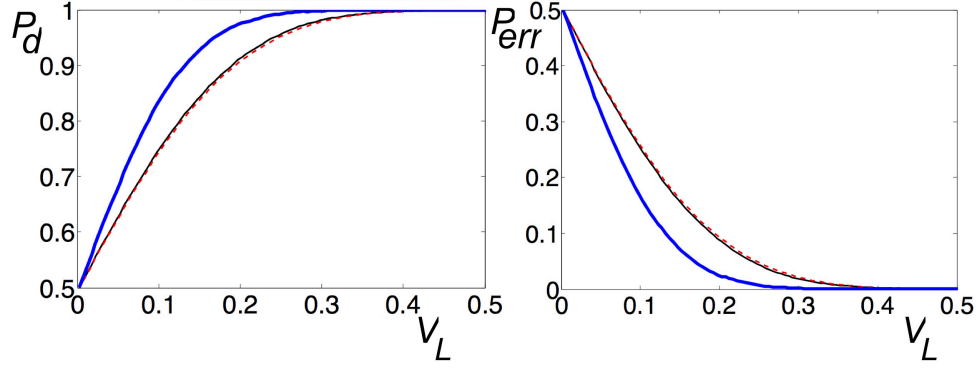


Figure 2: (Color online.) Probability of intrusion detection (left panel) and false alarm probability (right panel) as a function of the jamming level (7). The noise variance is  $\sigma = 0.1$ . The thin black, red dashed and thick blue lines correspond to the legitimate imagers using two classical states (15) and (16), one entangled and one classical (13) and (15) and two entangled states 13) and (14) respectively. For  $V_L > 0.5$  there is no significant difference between imaging with classical and quantum states.

The states used by the legitimate imagers are changed at random. We assume that the intruder does not know which of them was chosen, as the states have maximally mixed reduced states and cannot be distinguished by any local measurement. Therefore, the states carrying the false part of the image the intruder resends are independent of the choice by the legitimate imagers. For given angles of the analysers, legitimate imagers observe two images that have the same contribution from the false image. The difference between these images allows them to recover the correct image.

As we have already mentioned, the legitimate imagers use states with maximally mixed reduced states. All two-photon polarisation states with maximal mixed reduced states can be transformed by local changes of bases to the following class known as Bell diagonal states [24, 25]

$$\rho_{BD} = \frac{1}{4} + \mu_x \sigma_x \otimes \sigma_x + \mu_y \sigma_y \otimes \sigma_y + \mu_z \sigma_z \otimes \sigma_z, \quad (12)$$

where  $\sigma_x, \sigma_y$  and  $\sigma_z$  are three Pauli matrices,  $\mathbf{1}$  is the identity matrix,  $\mu_x, \mu_y$  and  $\mu_z$  are real parameters for which (12) is positive semidefined. Examples of these states, that will be used are the following:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\leftrightarrow\rangle + |\uparrow\uparrow\rangle) \quad \text{for } \mu_x = \mu_y = \mu_z = 1/4, \quad (13)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\leftrightarrow\rangle - |\uparrow\uparrow\rangle) \quad \text{for } \mu_x = \mu_y = -\frac{1}{4}, \mu_z = \frac{1}{4}, \quad (14)$$

$$\omega_1 = \frac{1}{2}(|\uparrow\uparrow\rangle\langle\uparrow\uparrow| + |\leftrightarrow\leftrightarrow\rangle\langle\leftrightarrow\leftrightarrow|) \quad \text{for } \mu_x = \mu_y = 0, \mu_z = \frac{1}{4}, \quad (15)$$

$$\omega_2 = \frac{1}{2}(|\nwarrow\nwarrow\rangle\langle\nwarrow\nwarrow| + |\nearrow\nearrow\rangle\langle\nearrow\nearrow|) \quad \text{for } \mu_y = \mu_z = 0, \mu_x = \frac{1}{4}, \quad (16)$$

Here  $|\uparrow\rangle, |\leftrightarrow\rangle$  and  $|\nwarrow\rangle, |\nearrow\rangle$  denote the vertical, horizontal, diagonal and antidiagonal polarisation states respectively. The states (13) and (14) are entangled while the states (15) and (16) are classically correlated. The coincidence detection probability for (12) is given by

$$P_{BD} = \frac{1}{4} + \mu_x \sin(2\theta_1) \sin(2\theta_2) + \mu_z \cos(2\theta_1) \cos(2\theta_2). \quad (17)$$

The visibility difference  $d$  (7) and the detection probability (5) depend on the intruder's set of possible states. We assume that this set is given by (12). For pairs of states from the set (13)-(16) the probability of detection is plotted in the left panel of Fig. 2 in the worst case scenario for different values of the level of jamming (9), while the probability of false detection is plotted in the right panel. The value of the noise variance is chosen to be  $\sigma = 0.1$ . For pairs of entangled states the detection probability is larger than for pairs of classically correlated states. In particular, for a level of jamming  $V_L = 0.1$  the probability of jamming detection is about 0.82 when two classical states are used

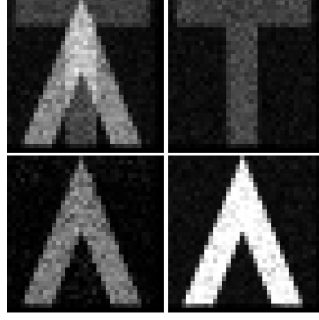


Figure 3: The upper left image shows the mixture of the correct ( $\Lambda$ -shape) and the false ( $T$ -shape) image obtained using states (13) and (15) respectively. The upper right image shows the false image. In this case, the correct part disappears because the legitimate states (14) are blocked by the polarisers. The lower left image shows the recovered image. For comparison, the lower right image shows the image without jamming.

for legitimate imaging while  $P_d = 0.92$  if entangled states are used. Preliminary numerical calculations show that the situation does not change in the intruder's favour if the intruder changes local bases of states (12). However, this analysis requires further investigation.

## 4.2 Jamming detection probability and recovery protocol - example

A simulation of an example of the recovery protocol is illustrated in figure 3. Here, we assume that in order to image a correct  $\Lambda$ -shaped object legitimate imagers use two classes of photons characterised by maximally entangled polarisation states  $|\psi_1\rangle$  and  $|\psi_2\rangle$  given by (13) and (14) respectively. During this process intercept-resend jamming occurs with intercepting rate  $r = 0.5$ . A false  $T$ -shaped image is imposed on the correct one. In this example we study a classical attack in which the false image is formed by photons in a classically correlated polarisation state  $\rho^E = \omega_1$  given in (15). The number of photons used in the simulation in order to form one image in a unit of time is  $n = 10^5$ . We assume that the detectors that are used for imaging record accidental counts, dark counts and other events that contribute to general noise at rate  $10^4$  for the unit of time across all pixels, i.e. 10% of the number of photons.

The legitimate imagers chose polariser angles  $\theta_1 = \theta_2 = \pi/4$ . The probability of the photons being detected are given by Eq. (17). This choice of angles provides the maximum state dependent visibility for imaging without jamming

$$V(\rho_1, \rho_2, \{\theta_i\}) = 1, \quad (18)$$

where  $\rho_1 = |\psi_1\rangle\langle\psi_1|$  and  $\rho_2 = |\psi_2\rangle\langle\psi_2|$ . The maximum value means that a correct image completely disappears when the state of the imaging photons is changed from  $\rho_1$  to  $\rho_2$ , as visualised in the upper panels of figure 3.

To estimate the probability of jamming detection we also calculate the state dependent visibility for jammed states  $\rho'_1 = (1-r)\rho_1 + r\rho^E$  and  $\rho'_2 = (1-r)\rho_2 + r\rho^E$ . Here we calculate this quantity for the central region of the image in which a part of the false 'T' is superimposed on the correct ' $\Lambda$ '. The visibility is

$$V(\rho'_1, \rho'_2, \{\theta_i\}) = 0.5 \quad (19)$$

and it can be measured experimentally. For an assumed variance of Gaussian noise  $\sigma = 0.1$  the difference between the visibility without intrusion and the one with jamming in units of  $\sigma$  is  $d = 5$  which guarantees that we detect the intrusion almost with certainty ( $P_d \approx 1$ , see (5)).

According to the recovery protocol the correct image is obtained as the difference between two images from the upper panels of figure 3. The recovered image is shown in the lower right panel of this figure, while in the lower left panel we show the correct image obtained without jamming.

During the imaging process random external noise independent of the image is recorded by detectors. We can observe that the noise level is reduced as an effect of our recovery protocol. Let us compare the levels of noise on two lower images of figure 3. The average amount of dark counts per pixel is about 8.7 for the chosen unit of time in the lower right panel. The level of noise in the case of the recovered image (the lower left panel) is about 5. The ratio between the average brightness of the  $\Lambda$ -shaped area and the noise without jamming is about 14 while for the recovered image this ratio is about 12. In consequence, the reduction of the absolute level of noise is observed in the simulation as

an effect of the recovery protocol. The relative noise is increased due to a difference in brightness between the images observed with or without jamming.

## 5 Concluding remarks and extensions

Imaging in which an imager controls the signal used to test a remote object is more robust than imaging relying on the signal coming from the object or from an uncontrollable source. This control gives us the ability to detect jamming and eliminate the jammed part of the image. We describe a detection and recovery protocol relying on the control of the polarisation of light. The protocol can be applied to negate the effect of jamming by a malevolent party as well as reducing the impact of background noise and signals on the imaging. Security of this protocol is provided by the fundamental fact that the party who prepares quantum states has more information about the states than it is possible to extract from a measurement. This creates an informational advantage of the legitimate imager with respect to an intruder. The latter cannot perfectly correlate the false image carrying states of light with the states from a legitimate source. As a consequence, the informational advantage can be used for false image detection and correct image restoration, as is done in our protocol.

In the description of our protocol we assumed that the state of the intruder is stationary during the imaging process, at least on average. This is a reasonable consequence of the assumption that the intruder does not distinguish between states from the legitimate source and create correlations with the changes of these states. Let us consider the situation in which this assumption is relaxed allowing for partial correlations between the intruder's states and the states from the legitimate source. Even in this case we are able to recognise the false contribution. It is enough to observe an image that appears when a filter at the legitimate detector completely blocks one of the legitimate states. This situation is shown in the upper right panel of fig. 3. The false image contribution still appears there. In this case, however, we cannot use simple difference between two images corresponding to different legitimate states to recover the correct image, since the brightness of the false image is now different on each of them. On the other hand, a modification of the protocol, taking a weighted difference between the two images is still possible, which will allow us to correct for this problem.

Free space application of the light beams together with the necessity of preservation of (or at least controlled interaction with) their polarisation states during imaging influences the conditions under which the protocol is applicable. In particular, the distance of the imaging is limited. Therefore, protocols like this one may not necessarily be considered in the context of radar type imaging of remote unknown objects. Instead, as the robots and drones industry is rapidly developed [26] they can be parts of modern surveillance systems with application of such proxy observers sent to vulnerable places of an area being protected. In this example readout of the device is more trusted if controlled states of light are used instead of the signal sent from the device in the border region between protected and uncontrollable areas. The protocol can be also used when the robot is sent to view an object in a noisy environment, where direct imaging is impossible. Another range of possible applications appears in the context of the general free space optical communication [27].

Correlation imaging can provide further information. For example, due to timing information we can confirm if beam path lengths are equal or have been changed as a consequence of jamming. We have shown here a further example of the advantage to be gained by using quantum over classically correlated states in coincidence ghost imaging.

We have discussed the situation in which jamming photons were directed to the detectors through the analysing polarisers. One alternative available to the intruder is jamming in which these photons are sent directly to the detectors side-stepping the polarisation analysers. Then the probability of detection does not depend on the polarisation states. As the intruder cannot optimize over these states the probability of intrusion detection is larger than in the case of jamming through the analysers, so this is not a useful intrusion strategy.

**Acknowledgements** The work was supported by the QuantIC Project of the UK Engineering and Physical Sciences Research Council (EP/M01326X/1). The authors thank Mehul Malik for useful discussion of an early version of this work and Masahide Sasaki for pointing out possible applications.

## References

- [1] T. B. Pittman, Y. H. Shih, D. V. Strekalov, and A. V. Sergienko, *Phys. Rev. A* **52**, R3429 (1995).
- [2] M. I. Kolobov, *Rev. Mod. Phys.* **71**, 1539 (1999).
- [3] L. A. Lugiato, A. Gatti, E. Brambilla, *J. Opt. B: Quantum Semiclass. Opt.* **4**, S176 (2002).

- [4] V. Giovannetti, S. Lloyd, and L. Maccone, *Science* **306**, 1330 (2004).
- [5] C. A. Santivanez, S. Guha, Z. Dutton, M. Annamalai, M. Vasilyev, B. J. Yen, R. Nair, J. H. Shapiro, *Proc. SPIE* 8163, *Quantum Communications and Quantum Imaging IX*, 81630Z (2011).
- [6] K. Jiang, H. Lee, C. C. Gerry, and J. P. Dowling, *J. Appl. Phys.* **114**, 193102 (2013).
- [7] M. Malik, O. S. Magaña-Loaiza, and R. W. Boyd, *Appl. Phys. Lett.* **101**, 241103 (2012).
- [8] T. S. Humble, R. S. Bennink, W. P. Grice, and I. J. Owens, *Intrusion Detection with Quantum Mechanics: A Photonic Quantum Fence*, 26. Army Science Conference; Orlando, FL (United States); 1-4 Dec 2008.
- [9] C. Bennett, and G. Brassard, in *Proceedings of IEEE International Conference CSSP*, Bangalore, India, p. 175 (1984).
- [10] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
- [11] N. Lütkenhaus, *Phys. Rev. A* **61**, 052304 (2000).
- [12] C. F. Sabottke, C. D. Richardson, P. M. Anisimov, U. Yurtsever, A. Lamas-Linares, and J. P. Dowling, *New J. Phys.* **14**, 043003 (2012).
- [13] T. S. Humble, R. S. Bennink, W. P. Grice, and I. J. Owens, *Proceedings of the SPIE*, **7342**, 73420H (2009).
- [14] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *J. Cryptology* **5**, 3 (1992).
- [15] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [16] B. I. Erkmen, and J. H. Shapiro, *Adv. Opt. Photon.* **2**, 405 (2010).
- [17] K. W. C. Chan, M. N. OSullivan, and R. W. Boyd, *Phys. Rev. A* **79**, 033808 (2009).
- [18] R. S. Aspden, N. R. Gemmell, P. A. Morris, D. S. Tasca, L. Mertens, M. G. Tanner, R. A. Kirwood, A. Ruggeri, A. Tosi, R. W. Boyd, G. S. Buller, R. H. Hadfield, and M. J. Padgett, *Optica* **2**, 1049 (2015).
- [19] R. S. Bennink, S. J. Bentley, and R. W. Boyd, *Phys. Rev. Lett.* **89**, 113601 (2002).
- [20] H. L. Van Trees, *Detection, Estimation, and Modulation Theory, Part I*, John Wiley & Sons, Inc., New York (2001).
- [21] T. S. Han, H. Endo, and M. Sasaki, *IEEE Trans. Information Theory* **60**, 6819 (2014).
- [22] D. V. Strekalov, A. V. Sergienko, D. N. Klyshko, and Y. H. Shih, *Phys. Rev. Lett.* **74**, 3600 (1995).
- [23] E.-K. Tan, J. Jeffers, S.M. Barnett, and D.T. Pegg, *Eur. Phys. J. D* **22**, 495, (2003).
- [24] B. Dakić, V. Vedral, and Č. Brukner, *Phys. Rev. Lett.* **105**, 190502 (2010).
- [25] R. Horodecki, and M. Horodecki, *Phys. Rev. A* **54** 1838 (1996).
- [26] M. Joel, *The Booming Business of Drones*, Harvard Business Review Jan 4, 2013.
- [27] F. J. Lopez-Martinez, G. Gomez, J. M. Garrido-Balsells, *IEEE Photonics Journal*, **7**, 1 (2015).